UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/664,893	09/19/2000	John Michael Everson	30604	5121

33272 7590 07/03/2006

SPRINT COMMUNICATIONS COMPANY L.P.
6391 SPRINT PARKWAY
MAILSTOP: KSOPHT0101-Z2100
OVERLAND PARK, KS 66251-2100

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 07/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/664,893
Filing Date: September 19, 2000
Appellant(s): EVERSON ET AL.

Mark L. Mollon
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 04 May 2006 appealing from the Office action mailed 26 January 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,199,113	Alegre et al	3-2001
5960411	Hartman et al	9-1999
6539482	Blanco et al	3-2003

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 112

In response: Applicant's arguments, see Page 6 – 8, filed on 4/5/2006 (Appeal Brief), with respect to Claims 1 – 12 and 21 – 36 have been fully considered and are persuasive. The rejection of Claims 1 – 12 and 21 – 36 has been withdrawn.

Claim Rejections - 35 USC § 102

Claims 1 – 4, 7 –10, 21, 24, 27, 29, 30, 32, 34 and 35 are rejected under 35 U.S.C. 102(e) as being anticipated by Alegre et al. (U.S. Patent Number 6,199,113).

Regarding Claim 1, Alegre teaches and describes

storing security information for a plurality of computer users in a user profile database (Column 4 lines 8 – 36);

the user launching a first secured computer application on an application server (Column 4 lines 8 – 36);

receiving at an authorization server coupled with the user profile database log-in information from the computer user who has launched a computer application (Column 4 lines 8 – 40);

in response to step b, creating a Session ID for the computer user with the authorization server (Column 4 lines 8 – 40 and Column 6 lines 24 – 42);

storing at least a portion of the Session ID on the user's computer (Column 4 lines 8 – 42);

also in response to step b, creating an object associated with the computer user or the Session ID (Column 4 lines 8 – 42 and Column 5 lines 8 – 20);

storing the object dynamically in a directory stored in a directory server coupled with the authorization server and the application server (Column 5 line 48 – Column 6 line 49);

copying at least some of the security information relating to the computer user from the user profile database to the object in the directory (Column 6 lines 24 – 67);

comparing the log-in information entered by the computer user to the security information for the computer .user and allowing the computer user access to the first

secured computer application if the user is an authenticated or authorized user of the first secured computer application (Column 6 lines 24 – 49); and

the user launching a second separately-secured computer application on an application server (Column 4 lines 48 – 67 and Column 8 lines 22 – 44);

the second separately-secured computer application reading the Session ID on the user's computer (Column 6 lines 6 – 68); and

the second separately-secured computer applications accessing the object for the computer user on the directory server in response to the Session ID to authenticate or authorize the user for the second separately-secured computer applications (Column 5 line 48 – Column 6 line 49).

Regarding Claim 7, Alegre teaches and describes

a user profile database for storing security information for a plurality of computer users (Column 4 lines 8 – 36);

an authorization server coupled with the user profile database for receiving log-in information from a computer user who has launched a first secured computer application, for creating a Session ID for the computer user, for storing at least a portion of the Session ID on the user's computer and for creating an object associated with the computer user or the Session ID (Column 4 lines 8 – 42; Column 5 lines 8 – 20 and Column 6 lines 24 – 42); and

a directory stored in a directory server coupled with the authorization server for dynamically storing the object created by the authorization server (Column 6 lines 24 – 34),

the authorization server being further operable for copying at least some of the security information relating to the computer user from the user profile database to the object in the directory, comparing log-in information entered by the computer user to the security information for the computer user and allowing the computer user access to the launched first secured computer application if the user is an authenticated or authorized user of the computer application (Column 5 line 48 – Column 6 line 49),

the directory server permitting other separately-secured computer applications launched by the computer user to reference the Session ID read by the separately-secured computer applications on the user's computer so that the other separately-secured computer applications may access the object for the computer user on the directory server to authenticate or authorize the user for the other separately-secured computer applications (Column 6 lines 6 – 67).

Regarding Claim 27, Alegre teaches and describes

the user remotely launching a first secured computer application from a user computer (Column 4 lines 8 – 36);

authenticating and authorizing the user to the first secured computer application by exchanging security information between the user and an authorization server (Column 5 line 48 – Column 6 line 49);

storing at least a portion of the security information in an object within a dynamic directory on a directory server (Column 5 line 48 – Column 6 line 49);

storing a link to the object on the user computer (Column 4 lines 25 – 54);

the user remotely launching a second separately-secured computer application on an application server (Column 4 lines 48 – 67 and Column 8 lines 22 – 44);

retrieving the link (Column 4 lines 25 – 54);

authenticating and authorizing the user to the second separately-secured computer application by exchanging the stored security information between the directory server and the application server (Column 5 line 48 – Column 6 line 49).

Regarding Claim 32, Alegre teaches and describes

an authorization server for authenticating and authorizing the user to secured computer applications by exchanging security information between the user and the authorization server when a first secured computer application is launched by the user (Column 5 line 48 – Column 6 line 49);

a directory server storing at least a portion of the security information in an object within a dynamic directory, wherein a link to the object is stored on the user computer; and

an application server implementing a second separately-secured computer application for remote launching by the user, wherein the second separately-secured computer application retrieves the link, and wherein the user is authenticated and authorized to the second separately-secured computer application by exchanging the

stored security information between the directory server and the application server(Column 5 line 48 – Column 6 line 67).

Claims 2 and 8 are rejected as applied above in rejecting claims 1 and 7. Furthermore, Alegre teaches and describes the security information including authentication and authorization information (Column 4 lines 48 – 67 and Column 7 lines 55 – Column 8 line 20).

Claims 4, 10, 29 and 34 are rejected as applied above in rejecting claims 1 and 7. Furthermore, Alegre teaches and describes the Session ID being based on at least one of the following: a date on which the computer user launched the first secured computer application; a time in which the computer user launched the first secured computer application; a TCP/IP address of the computer user; and a user name of the computer user (Column 3 lines 1 – 11, Column 5 lines 8 – 36 and Column 6 lines 24 – 68).

Claims 3 and 9 are rejected as applied above in rejecting claims 2 and 8. Furthermore, Alegre teaches and describes the authentication and authorization information including at least one of the following: user names, user IDs, passwords, public-key data, certificates, and access control information (Column 5 line 8 – Column 6 line 65).

Claims 21 and 24 are rejected as applied above in rejecting claims 1 and 7. Furthermore, Alegre teaches and describes wherein the other computer applications access the object on the directory server using a dynamic directory service (Column 5 line 48 – Column 6 line 49).

Claims 30 and 35 are rejected as applied above in rejecting claims 27 and 32. Furthermore, Alegre teaches and describes the steps of:

one of the secured computer applications storing application data in the object; and the other one of the secured computer applications retrieving the application data according to the link (Column 4 lines 32 – 67).

Claim Rejections - 35 USC § 103

Claims 5, 6, 11, 12, 31 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alegre et al. (U.S. Patent Number 6,199,113, hereinafter "Alegre") in view of Hartman et al. (U.S. Patent Number 5,960,411 hereinafter "Hartman").

Claims 5, 11, 31 and 36 are rejected as applied above in rejecting claims 1, 7 , 30 and 35. Alegre does not explicitly disclose that the method for dynamically tracking a user session includes the steps of creating a shopping cart and storing the shopping cart along with the object in the directory. However, Hartman discloses a method for creating a shopping cart and storing the shopping cart along with a unique client

identifier (cookie), purchaser-specific information (Hartman Column 3 line 31 – Column 6 line 21). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Hartman's shopping cart system into the dynamically tracking user session system of Alegre.

Alegre could have been modified by Hartman to arrive the claimed invention by having the shopping cart with user purchase information to be saved on the directory as taught by Hartman (See Hartman Column 3 line 31 – Column 8 line 25) and as suggested by Alegre (See Alegre Column 7 line 3 – Column 8 line 53). One of ordinary skill in the art would have been motivated to modify Alegre by Hartman as discussed above because in a shopping cart systems user profiles are stored in a directory as taught by Hartman and employing the shopping cart within Alegre would provide an efficient and secure method for dynamically tracking a user session.

Claims 6 and 12 are rejected as applied above in rejecting claims 5 and 11. Furthermore, Alegre teaches and describes the steps of allowing the user to select items to be purchased and storing information relating to the selected items in the shopping cart (Hartman Column 3 line 46 – Column 4 line 26; Column 5 line 27 – Column 6 line 21 and Column 7 line 57 – Column 8 line 25).

Claims 22, 23, 25, 26, 28 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alegre et al. (U.S. Patent Number 6,199,113, hereafter "Alegre") in view of Blanco et al. (U.S. Patent Number 6,539,482, hereafter "Blanco").

Claims 22, 25, 28 and 33 are rejected as applied above in rejecting claims 21 and 24. Furthermore, Alegre teaches and describes wherein the other computer applications access the object on the directory server using a dynamic directory service (Column 5 line 48 – Column 6 line 49). Alegre does not explicitly disclose that the dynamic directory service comprises the lightweight directory access protocol (LDAP). However, Blanco discloses a network access authentication system that gathers the data concerning the users, including authentication data, in a data base of a directory, which uses Light weight directory access protocol which is specifically targeted at management applications and browsing applications that provide interactive access to directories (Blanco Column 3 lines 22 – 67).

Motivation to combine Blanco with Alegre comes from the need to provide authentication and authorization of a user available to an authorization server coupled with a directory server that stores the authentication (user) data. Alegre provides a discussion of the need for security and authorization information for all the resources that a user can access but is silent as to the specific details of the LDAP, see Alegre Column 1 line 51 – Column 2 line 35 (especially Column 2 lines 24 – 35). It would have been obvious to one of ordinary skill in the art to combine Alegre with Blanco because LDAP provides the authentication data stored in the directory available to all the applications that are associated with a directory server and provides interactive access to directories.

Claims 23 and 26 are rejected as applied above in rejecting claims 21 and 24. Furthermore, Alegre teaches and describes wherein the other computer applications access the object on the directory server using a dynamic directory service (Column 5 line 48 – Column 6 line 49). Alegre does not explicitly disclose that the dynamic directory service comprises the X.500 access protocol. However, Blanco discloses a network access authentication system that gathers the data concerning the users, including authentication data, in a data base of a directory, which uses Light weight directory access protocol that supports X.500 access protocol (Blanco Column 3 lines 22 – 67).

Motivation to combine Blanco with Alegre comes from the need to provide authentication and authorization of a user available to an authorization server coupled with a directory server that stores the authentication (user) data. Alegre provides a discussion of the need for security and authorization information for all the resources that a user can access but is silent as to the specific details of the LDAP, see Alegre Column 1 line 51 – Column 2 line 35 (especially Column 2 lines 24 – 35). It would have been obvious to one of ordinary skill in the art to combine Alegre with Blanco because LDAP which supports X.500 access protocol, provides the authentication data stored in the directory available to all the applications that are associated with a directory server and provides interactive access to directories.

(10) Response to Argument

(10 a) Regarding Claims 1, 7, 27 and 32, Applicant argues that Alegre et al does not disclose the following teachings "an object associated with the Session ID is stored dynamically in a directory on a directory server coupled with the authorization server", "user is authenticated **and** authorized to the first secured computer application to be launched by interacting with an authorization server", "user is authenticated **and** authorized to a second separately-secured computer application by accessing the object for the computer user on the directory server rather than requiring further interaction with the authorization server", "separately-secured computer applications that are remotely launched by a user", "using a directory to store an object accessed by more than one application for purposes of authentication", "multiple applications that each requires its own separate authorization", "authenticating a user to a remote application on an application server" and "does not provide any teaching to show what the additional access policies are".

In response: These arguments are not persuasive because: these above claim recitations used in the Applicant's arguments do not correspond to the amended claims filed on June 16, 2005.

With respect to the claim limitation "an object associated with the Session ID is stored dynamically in a directory on a directory server coupled with the authorization

server", **Attention is directed** to the **actual** Claim recitation, " creating an object associated with the computer user **or** the Session ID, and ""storing at least a portion of the security information in an object", (**emphasis added**). Claim limitation requires creating an object associated with **either** the user **or** the Session ID. Applicant's disclosure on page 6 lines 14 – 28, defines an object representing the user in the form cookie **or** Session ID and further discloses that Session ID may relate to the date or time that the user logged in, the media access control (MAC) address of the user's computer, the TCP/IP address of the user's computer, the user's name, an account code for the user, a combination of any of these criteria, or any other criteria.

Alegre discloses an authentication server requesting a session key from a key server, which creates a session key (**object**) and storing the session key along with the user ID and PWD. Alegre also discloses creating a cookie (**object**) associated with the computer user, which is placed in the user's computer by storing cookies (small files used to store the session key placed on a user's computer by a server) and using such session key to request (access) for other resources on network. (See Alegre Column 4 lines 8 – 42; Column 5 lines 8 – 20; Column 6 lines 24 – 67 and Column 7 line 1 – Column 8 line 27).

With respect to the claim limitation "user is authenticated **and** authorized to the first secured computer application to be launched by interacting with an authorization server", **Attention is directed** to the **actual** Claim recitation, "comparing log-in information entered by the computer user to the security information of for the

computer user and allowing the computer user access to the first secured computer application if the user is an authenticated **or** authorized user of the first secured computer application to be launched by interacting with an authorization server" (**emphasis added**). Contrary to Applicant's arguments, the Claim limitation requires authenticated **or** authorized user but not both.

However, Alegre discloses that the first time a user requests access to a resource on the trusted network, only after determining validity of the user ID and password (authentication), a Session ID is created. Subsequently, the session key is transmitted with the user access request so that the trusted network can use the session key to authenticate the user and access resources on network, depending upon access levels (authorization) corresponding to each particular user. (See Alegre Column 4 lines 8 – 42; Column 5 lines 8 – 20; Column 6 lines 24 – 67 and Column 7 line 1 – Column 8 line 27). Alegre's "user associated with particular level of access permission" is interpreted as "user authorization".

With respect to the claim limitation "user is authenticated **and** authorized to a second separately-secured computer application by accessing the object for the computer user on the directory server rather than requiring further interaction with the authorization server", **Attention is directed** to the **actual** Claim recitation "the second separately-secured application accessing the object for the computer user on the directory server in response to the Session ID to authenticate **or** authorize the user for the second separately-secured computer application" (**emphasis added**). Contrary to

Applicant's arguments, the Claim limitation requires authenticated **or** authorized user to a second separately-secured computer application but not both.

Alegre discloses user access to a particular level of information (authorization) and level access information to be included in the user profile that specifies user's access rights (authentication **or** authorization) to trusted network. Alegre further discloses in response to (valid) Session key (Session ID), the trusted network performs one or more of the network resources (second separately-secured application) access request. (See Alegre Column 4 lines 8 – 42; Column 5 lines 8 – 20; Column 6 lines 24 – 67 and Column 7 line 1 – Column 8 line 27) and **With respect to** "separately-secured computer applications that are remotely launched by a user", **Attention is directed** to Alegre Fig. 2; Column 4 lines 8 – 16 and Column 8 lines 21 – 27, wherein the user remotely requests (launches) for one or more operations by resources, which is interpreted as separately-secured computer applications on network.

With respect to "using a directory to store an object accessed by more than one application for purposes of authentication", **Attention is directed** to Alegre Column 6 lines 23 – 42 and Column 8 lines 8 – 44, wherein Authentication server (database/directory) stores user profile (object representing user's information such as cookie), that specifies user's access rights associated with each user has to the resources (applications) along with the access profile and the access request from the speaker object (session key). Applicant's disclosure on page 6 lines 14 – 28 and lines

50 – 67, defines a directory as "to store dynamic information such as session information".

Alegre discloses storing User profile (object) on the database and further discloses storing Session key (object), user profile (object) on the key server (database). Furthermore, Alegre discloses the key server permits the user to access network resources (more than one application) by checking the authentication of the stored object (user profile or Session key). Thus Alegre discloses that the object stored in the database is used for the purpose of authentication.

With respect to and "multiple applications that each requires its own separate authorization". **Attention is directed** to Alegre Column 8 lines 8 – 44, wherein the user request may include one or more requests for resources (multiple applications) and the level access information (separate authorization) is included in the user profile that may define a variety of access permits other acceptable operations by the user.

With respect to the claim limitation "authenticating a user to a remote application on an application server", **Attention is directed** to Alegre Column 4 lines 55 – 63, wherein the key server permits the user (client 110) to access network resources (more than one application) by checking the authentication of the stored object (user profile or Session key) and these applications are on a remote application server (DB server 142 and DB 134 on the trusted network).

With respect to the argument "does not provide any teaching to show what the additional access policies are", Alegre discloses additional access policies such as Firewall (118) for providing security, Database server (142) performing security checks and creating a unique and unpredictable session key), see Column 2 lines 3 – 23 and Column 4 lines 37 – 42).

(10 b) Regarding Claims 5, 6, 11, 12, 31 and 36, Applicant argues that Hartman et al does not disclose "the directory objects or the authentication and authorization of a plurality of remote applications by linking to the directory objects" and "a shopping cart with a directory object that can be used by a plurality of applications". Applicant further argues that Hartman or Alegre do not provide any motivation to one skilled in the art to associate a shopping cart with a directory object that can be used by a plurality of applications.

In response: These arguments are not persuasive because:

With respect to "the directory objects or the authentication and authorization of a plurality of remote applications by linking to the directory objects", Hartman et al was not combined with Alegre to show "the directory objects or the authentication and authorization of a plurality of remote applications by linking to the directory objects". In fact, Claims 5, 6, 11, 12, 31 and 36, do not recite "the directory objects or the authentication and authorization of a plurality of remote applications by linking to the directory objects".

With respect to "a shopping cart with a directory object that can be used by a plurality of applications", **Attention is directed** to the **actual** Claim recitation "**creating a shopping cart and storing the shopping cart along with the object in the directory**" and "**allowing the user to select items to be purchased and storing information relating to the selected items in the shopping cart**" (**emphasis added**). Hartman discloses, specifically creating a shopping cart and providing user with a cookie to identify and store information related the user and order information (items in the shopping cart) wherein purchase information associated with the user is stored on the server Column 4 lines 9 – 26 and Column 6 lines 12 – 21.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Alegre provides the teachings for storing user profile along with authentication and authorization (to access multiple applications) on a server and anticipates using the user profile to access web pages (Alegre Column 8 lines 54 – 65) wherein Hartman discloses a shopping cart via web pages while storing a cookie on the client (user) system to track user transactions.

(10 c) Regarding Claims 22, 23, 25, 26, 28 and 33, Applicant argues that Blanco does not use LDAP or x.500 to access objects having the limitations recited in the present claims.

In response: This argument is not persuasive because:

With respect to Blanco's teachings, an authentication system uses the **L**ight **w**eight **D**irectory **A**ccess **P**rotocol (**LDAP**) with a directory supporting **X.500** protocol to authenticate a remote user (Blanco, specifically, Column 3 lines 24 – 37 and Column 4 lines 40 – 63).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Pramila Parthasarathy

Conferees:

Gilberto Barron

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Benjamin E. Lanier